UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,607	06/01/2001	Christophe Clavier	1032326-000132	2078

21839 7590 09/16/2009

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
09/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	09/807,607	CLAVIER ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on June 5, 2009. Claims 1-10, and 13-16 were previously pending consideration. No claims were cancelled or added by virtue of the received amendment.

2. Claims 1-10, and 13-16 are currently being considered.

Response to Arguments

Applicant's arguments filed June 5, 2009 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 13, the Applicant argues that the Cited Prior Art (CPA), Leppek (U.S. Patent 5,933,501), does not teach a means for generating a random value for selecting an encryption means to be employed during a given execution of an algorithm. This argument is not found persuasive. The CPA teaches a key which is used to determine which sequence of encryption operators will be used. The key itself is a random value which can vary as desired (column 2, lines 50-55), and as a result, this random key causes the supervisory module to create a random sequence of encryption operators (column 4, lines 33-38). Therefore, the arguments are not found persuasive, and the rejection is maintained as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 13 is rejected under 35 U.S.C. 102(e) as being anticipated by Leppek (U.S. Patent 5,933,501).

Regarding claim 13, Leppek discloses:

An electronic component which provides countermeasure against attacks on a secret key cryptographic algorithm, comprising:

a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data (column 1 line 63 – column 2 line 5), *wherein a encryptor operator database stores different encryptor operators*;

a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means (column 4, lines 24-32), *based on the address codes selected a combination of encryption operators (manipulating means) are applied to the data*; and

means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced is

thereby unpredictable (column 4, lines 33-38), *wherein a key (random value) is supplied to encryption assembly manager which comprises address code sequences which are used to form the combination of the encryption operators into a unique sequence (manipulating means) which is then applied to the data.*

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Leppek discloses:

The electronic component of claim 13 wherein said different manipulating means respectively produce sets of output data that are complementary to one another (column 6, lines 4-14), *wherein a complementary virtual schemes can be used.*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent 5,933,501) in view of Kocher (U.S. Patent 6,278,783).

Claim 14 is rejected as applied above in rejecting claim 13. Leppek does not explicitly teach wherein said manipulating means are a table of constants. Kocher discloses that manipulating means are constants tables (column 7, lines 15-65). Kocher

teaches the uses of tables to manipulate data. These tables are filled with parameters (constants) that are updated so that attackers cannot obtain the contents of the table by an analysis of measurements. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the tables of constants to minimize information leakage when using an electronic component such as a smart card (Kocher: Abstract).

Claim 16 is rejected as applied above in rejecting claim 13. Leppek does not explicitly disclose that the electronic component is a smart card. Kocher teaches the use of smart cards in preventing leakage of information (Kocher: see Abstract). Leppek teaches that the information is sent from a user workstation over a network (Leppek: column 1, lines 31-38). It would have been obvious to implement the system of Leppek on a smart card because smart cards are portable.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
09/07/2009

Primary Examiner, Art Unit 2431